Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

COMMENTS OF COMCAST CORPORATION

Matthew A. Brill
Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

July 3, 2017

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

COMMENTS OF COMCAST CORPORATION

Comcast Corporation ("Comcast") submits these comments in response to the Notice of Proposed Rulemaking and Notice of Inquiry adopted on March 23, 2017 in the above-captioned proceeding.[1]

INTRODUCTION AND SUMMARY

Comcast applauds the Commission's ongoing efforts, in partnership with industry stakeholders, to combat illegal robocalls that rely on "spoofed" caller ID information designed to mislead consumers and lure them into scams. These robocalls cause significant harm to Comcast's customers and other consumers. Bad actors increasingly are able to "use cheap and accessible technologies" to mask or alter their caller ID information, and to "scam victims with threats from the IRS, offers of loans, or free travel."[2] Illegal spoofed robocalls also can "lead[] to identity theft," often perpetrated by scammers posing as legitimate businesses with which the

---

1 *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 17-24 (rel. Mar. 23, 2017) ("*Robocall Blocking NPRM/NOI*" or "Notice").

2 *See* Robocall Strike Force, *Robocall Strike Force Report*, at 1 (rel. Oct. 26, 2016), *available at* https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf ("Oct. 2016 Strike Force Report").

recipient of the call has an existing relationship.[3] Additionally, these robocalls impose substantial network costs on Comcast and other providers of voice services. According to one industry estimate, "[o]ver 42 percent of all calls made to landlines are . . . illegal unwanted robocalls,"[4] and in Comcast's experience, a substantial portion of these calls appear to involve the use of spoofed caller ID information.

Comcast is proud to be a leader in industry efforts to combat these abusive practices. Comcast's Chris Wendt co-chairs the work group of the Alliance for Telecommunications Industry Solutions ("ATIS") on the SHAKEN (Signature-based Handling of Asserted Information Using toKENs) framework for caller ID authentication, is a primary author of the STIR (Secure Telephone Identity Revisited) specifications adopted by the Internet Engineering Task Force ("IETF"), and leads the development team pioneering an open source implementation of the specifications to promote testbeds and interoperability lab trials in the industry.[5] Comcast has also provided open source code for implementation of SHAKEN and STIR that vendors and other providers of voice services have begun to use.[6]

Additionally, Comcast was an active member of the Robocall Strike Force, which was organized in 2016 "to accelerate the development and adoption of new tools and solutions to

---

3 *See Robocall Blocking NPRM/NOI* ¶ 1.

4 Rebecca Russell, *Spike in "Robocalls" Reported Across the Country*, Fox 17 Online, May 16, 2017, *available at* http://fox17online.com/2017/05/16/spike-in-robocalls-reported-across-the-country/ (quoting Aaron Foss, founder of Nomorobo).

5 Mr. Wendt also recently received the ATIS President's Award recognizing his critical work with ATIS in mitigating unwanted robocalling and caller ID spoofing. *See* Marcella Wolfe, *ATIS Awards Honor Members' Visionary Leadership and Industry Contributions,* ATIS (May 9, 2017), https://sites.atis.org/insights/atis-awards-honor-members-visionary-leadership-industry-contributions/.

6 *See* "Secure Telephone Identity Management in Session Initiation Protocol," https://github.com/Comcast/vesper.

abate the proliferation of illegal and unwanted robocalls" and "to promote greater consumer control over the calls they wish to receive."[7] Mr. Wendt co-chaired the Strike Force's Authentication Work Group, which aimed to advance the development of "standards to verify and authenticate caller identification for calls carried over an Internet Protocol ('IP') network."[8] The Strike Force issued an initial report in October 2016 presenting its findings and making recommendations for "actions the FCC can take to support industry efforts to trace back and to block illegal robocalls,"[9] and published another report describing further industry efforts in April 2017.[10]

Comcast also has been and continues to be an active participant in the "Do-Not-Originate" ("DNO") trial that significantly curbed the number of consumer complaints associated with the widely reported scam involving the spoofing of numbers belonging to the IRS, discussed further below in Section I.B. And as a further effort to empower consumers to prevent illegal robocalls, Comcast offers Nomorobo[11] compatibility with its residential voice product, XFINITY Voice, and provides information on its website about how to activate Nomorobo in conjunction with its voice service.[12] XFINITY Unlimited customers also can

---

7 Oct. 2016 Strike Force Report at 1.

8 *Id.* at 4.

9 *Id.*

10 *See* Robocall Strike Force, *Industry Robocall Strike Force Report*, at 1 (rel. Apr. 28, 2017), *available at* https://www.fcc.gov/file/12311/download ("Apr. 2017 Strike Force Report," and together with the Oct. 2016 Strike Force Report, the "Strike Force Reports").

11 Nomorobo is a third-party cloud-based service that can block certain robocalls.

12 *See* Comcast Corp., "How to Stop Unsolicited Robocalls to Your Home," https://www.xfinity.com/support/phone/nomorobo/.

choose to activate call control tools, including call screening and anonymous call rejection. Comcast provides each of these tools at no additional cost to end users.

As an industry leader in this arena, Comcast has been encouraged by the Commission's early attempts to facilitate the blocking of unwanted robocalls—first by affirming in 2015 that voice providers may "implement[] call-blocking technology and offer[] consumers the choice . . . to use such technology,"[13] and then by clarifying in 2016 in a staff-level Public Notice that "voice service providers may block . . . calls" using a spoofed caller ID number "when requested by the spoofed number's subscriber."[14] The Commission's *Robocall Blocking NPRM/NOI* represents another laudable step toward exploring reasonable and balanced measures that would enable voice providers to take action to curtail illegal spoofed robocalls, while at the same time protecting consumers from overzealous call blocking that may prove to be more harmful than helpful.

Comcast welcomes the opportunity to comment on these proposals, and believes the Commission will benefit from hearing from stakeholders on the merits (and, in some cases, potential pitfalls) of the mitigation techniques raised in the *Robocall Blocking NPRM/NOI*. To be sure, as the Strike Force Reports point out, "there is no single 'silver bullet' to the robocall problem."[15] But Comcast believes that pursuing the following initiatives in the manner set forth herein could help significantly curtail illegal spoofed robocalls:

---

13 *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, 30 FCC Rcd 7961 ¶ 154 (2015).

14 *Consumer and Governmental Affairs Bureau Clarification on Blocking Unwanted Robocalls*, Public Notice, 31 FCC Rcd 10961, 10962 (CGB 2016) ("*2016 Guidance PN*").

15 Apr. 2017 Strike Force Report at 25.

- Although the Notice does not propose any concrete rules around SHAKEN and STIR implementation, the Commission should be doing everything in its power to facilitate the development and adoption of these IP-based authentication standards—including by speeding along the IP transition and adopting safe harbors for providers that adopt the standards. Once these standards are in place and broadly adopted, voice providers will be able to identify a large number of illegitimately or fraudulently spoofed calls quickly and accurately, thus potentially obviating the need for call-blocking based solely on whether the number is unassigned.

- The Commission also should take steps to facilitate the ability of voice providers to develop and implement other tools for identifying and blocking illegal spoofed robocalls, including traceback and Do-Not-Originate capabilities. Comcast supports the adoption of regulatory safe harbors for: (1) providers that employ these tools, including the proposal to codify the *2016 PN Guidance*; and (2) other filtering methodologies and approaches to cover as-yet undeveloped technologies. Comcast knows from its more than 15 years battling email spam, phishing, and malware that the effectiveness of certain measures will change rapidly over time and that new defenses will be required.

- Finally, Comcast supports the Commission's proposal to establish a safe harbor enabling voice providers to block robocalls where the spoofed number is invalid under the North American Numbering Plan ("NANP"), as set forth in Appendix A to the Notice. And Comcast is open to working with the Commission and stakeholders on exploring the viability of the other proposed rules in Appendix A—namely, to enable blocking of valid but unallocated numbers and blocking of allocated but unassigned numbers—though these proposals present potentially significant practical concerns (such as the need to unblock numbers as they are allocated and assigned) that the Commission should account for and address before adopting such rules.

Pursuing the approach set forth in these comments will represent a major step forward in the Commission's efforts to empower voice providers and consumers to take action against illegal spoofed robocalls. Comcast is eager to continue this important work with the Commission and other stakeholders.

I. THE COMMISSION SHOULD PROMOTE THE USE OF OBJECTIVE CRITERIA TO IDENTIFY AND ADDRESS ILLEGAL SPOOFED ROBOCALLS

While the *Robocall Blocking NPRM/NOI* begins with a discussion of proposals to allow blocking of invalid, unallocated, and unassigned numbers, discussed further in Section II, *infra*, the more promising and comprehensive initiatives for mitigating illegal robocalling appear later in the Notice—particularly in the discussion of the SHAKEN and STIR standards for caller ID

authentication currently under development.[16] As discussed herein, the SHAKEN and STIR framework currently represents the most promising avenue for addressing illegal spoofed robocalls in a holistic manner, and the Commission should provide regulatory protections for voice providers that employ this framework to block such calls.[17] Because these standards are largely reliant on IP-based standards, the Commission also should do everything it can to facilitate the transition to IP-based networks, which in turn will facilitate IP-to-IP interconnection and enable widespread adoption and implementation of SHAKEN and STIR. Moreover, as noted below, the Commission should adopt measures that promote other techniques to identify and block illegal spoofed robocalls based on objective criteria.

A. The Commission Should Focus on Paving the Way for Broad Adoption of SHAKEN and STIR Authentication Standards

As the Commission appropriately recognizes, standards bodies and various industry participants, including Comcast, have made "significant progress on Caller ID Authentication Standards" that can play a key role in identifying and addressing illegal spoofed robocalls—most

---

16 *Robocall Blocking NPRM/NOI* ¶ 32.

17 As a threshold matter, the Commission should focus its efforts primarily on robocalls for which the caller ID information has been spoofed without any legitimate purpose. *Cf. Robocall Blocking NPRM/NOI* ¶ 5 (providing examples of the legitimate alteration of caller ID information, such as where "a domestic violence shelter seek[s] to protect victims who make calls" or where "doctors want[] to display their main office number"). Proposals to define "illegal robocall" more broadly, such as the suggestion that providers could block any call that violates the Telephone Consumer Protection Act ("TCPA") and the Commission's implementing rules, *id.* ¶ 13, likely would prove to be unadministrable. As the Commission is well aware, the question whether a particular call violates the TCPA is heavily fact-dependent—often turning on the content of the call, disputes over whether consent exists, the type of calling platform, and other issues. It would be impracticable and inappropriate for voice providers to try to determine the legality of a particular call under the TCPA as the call traverses its network. Rather than potentially hampering voice providers with an impracticable framework for determining what constitutes an "illegal robocall," the Commission's focus should be to equip voice providers with an array of tools to address plainly illegitimate robocalling practices, as discussed herein.

notably, the SHAKEN and STIR framework.[18] In a nutshell, the goal of SHAKEN and STIR is to provide a process whereby "telephone calls and the telephone numbers associated with the calls, when they are originated in a service provider network[,] can be authoritatively and cryptographically signed by the authorized service provider, so that as the telephone call is received by the terminating service provider, the information can be verified and trusted."[19] The STIR framework allows a provider to cryptographically sign, or attest to, calling party information at its origin and to verify this information at the call termination point; SHAKEN, in turn, defines a methodology for providers using STIR to communicate authentication information across networks.[20]

As explained in the Strike Force Reports, this framework "holds considerable promise for repressing the presence of robocalling in the communications ecosystem," as it will "provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end."[21] Moreover, the framework "has broad industry support, having been approved by both ATIS and SIP Forum under their respective transparent, consensus-based approval processes."[22] ATIS has created a Robocalling Test Bed that allows service providers and vendors to

---

18 *Robocall Blocking NPRM/NOI* ¶ 32.

19 Oct. 2016 Strike Force Report at 5.

20 *See* ATIS, *Developing Calling Party Spoofing Mitigation Techniques: ATIS' Role*, at 3-4 (Aug. 2016), https://www.atis.org/01_resources/whitepapers/ATIS_Robocalling_Summary.pdf.

21 Oct. 2016 Strike Force Report at 5. Notably, the SHAKEN and STIR framework also enables voice providers to distinguish fraudulently spoofed calls from calls where the caller ID information has been changed for legitimate reasons. In the latter context, the originator of the call would have an authenticated relationship with the service provider, allowing for "partial attestation" of the call in a manner that would signal that the call is legitimate.

22 Apr. 2017 Strike Force Report at 5.

experiment with and trial their implementations of SHAKEN and STIR in a test environment to ensure full interoperability.[23] ATIS membership is not required to participate; any service provider with an assigned Operating Company Number ("OCN") is eligible to use the test bed.[24] Other parties, such as equipment manufacturers, may participate as well if they have technological solutions relevant to the SHAKEN and STIR framework available to test.[25] These open testing processes have helped accelerate the development of the framework.

The SHAKEN and STIR framework relies on IP technology to transmit authentication information with each call, and therefore functions best for calls that originate and terminate in IP format. The specifications for SHAKEN and STIR *also* contemplate an authentication method for calls originated in time-division multiplexing ("TDM") format and exchanged in IP by creating and applying the digital signature at the gateway at which the call is converted to IP format.[26] This TDM authentication, however, is not as robust as it would be on an all-IP path, as it cannot verify with complete confidence that the caller ID information for a particular call was not altered before the call was converted to IP. Relatedly, while the SHAKEN and STIR framework does not require that *all* voice providers transition to IP in order for authentication to work for calls between *two* IP-based voice providers that have implemented the protocols, the framework naturally will not be a truly *nationwide* solution for end-to-end authentication until the ongoing IP transition is complete[27]—an outcome that the Commission should continue to

---

23 *Id.* at 6.

24 *Id.*

25 *Id.*

26 *See* Oct. 2016 Strike Force Report at 9.

27 ATIS has also developed and published a document providing operational guidance for interoperability with so-called Next Generation Network telephone service providers

speed along. Even so, the framework's reliance on IP should not prevent or delay Commission action to enable and facilitate implementation of the framework wherever possible.

Accordingly, the Commission should adopt a rule expressly authorizing voice providers to block unauthenticated calls where both the originating and terminating providers have implemented SHAKEN and STIR. Adopting such a clear and bright-line rule would encourage providers to implement SHAKEN and STIR, thereby helping to mitigate the possibility of dramatic increases in abusive call rates, while also offering providers the greatest assurance that their efforts would not disrupt legitimate calls or expose them to enforcement action. Relatedly, the Commission should establish a safe harbor for entities acting in good faith from enforcement actions for inadvertently blocking a legitimate call, as the Strike Force recommended,[28] and as the Notice proposes.[29] Absent a safe harbor, voice providers may be reluctant to implement reasonable robocall mitigation techniques that, while highly effective, may not be completely error-free and could otherwise expose providers to enforcement action for inadvertently blocked calls.

The Commission should also adopt its proposal—initially recommended by the Strike Force—not to count these blocked calls "for purposes of calculating a provider's call completion rate."[30] To be sure, the Commission's efforts to promote the completion of long-distance calls to

---

when implementing the SHAKEN framework and processing calls through their networks. *See* Apr. 2017 Strike Force Report at 5.

28 Oct. 2016 Strike Force Report at 36.

29 *Robocall Blocking NPRM/NOI* ¶¶ 34-36.

30 *Id.* ¶ 26. Voice providers generally are able to distinguish between calls that are blocked and calls that fail for other reasons (based on the use of unique error codes in call detail records).

rural areas serve important interests,[31] and the Commission is continuing to refine its approach in this arena.[32] But adopting the Commission's proposal not to count these blocked calls for purposes of calculating a provider's completion rate would not undermine those interests. Rather, exempting blocked calls from these calculations would avoid penalizing providers that seek to protect their customers from robocalls, and dispel any existing confusion as to whether blocking these calls somehow runs afoul of Commission requirements.

Finally, the Commission should adopt its proposal "not to require providers to obtain an opt-in from subscribers" in order to block such calls based on SHAKEN and STIR authentication.[33] As the Commission correctly notes, "no reasonable consumer would want to receive" illegal spoofed robocalls,[34] and there is rich literature in behavioral economics that explains at length why a default of opt-out is superior to opt-in in analogous cases.[35] Along these lines, the Commission should further clarify that voice providers retain flexibility in responding to subscriber requests, and may block other types of incoming robocalls when requested to do so by a subscriber (*e.g.*, certain fraudulent calls originated outside the United States, as discussed further in Section II, *infra*).

---

31 *See Rural Call Completion*, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154 ¶ 13 (2013) (noting that ensuring high rural call completion rates promotes "public safety" interests, among other things).

32 *See generally* Fact Sheet, *Rural Call Completion*, WC Docket No. 13-39 (rel. Jun. 22, 2017) (attaching a draft of a Second Further Notice of Proposed Rulemaking on rural call completion issues).

33 *Robocall Blocking NPRM/NOI* ¶ 25. At the same time, the Commission should not limit providers' flexibility in implementing opt-in or opt-out approaches to call-blocking as appropriate.

34 *Id.*

35 *See, e.g.*, Letter of Dr. Sara C. Wedeman, BECG, to Chairman Tom Wheeler *et al.*, WC Docket No. 16-106 (filed May 25, 2016); Letter of Dr. Sara C. Wedeman, BECG, to Chairman Tom Wheeler *et al.*, WC Docket No. 16-106 (filed May 27, 2016).

B. The Commission Also Should Facilitate the Use of Other Robocall Mitigation Tools Based on Objective Criteria

While the SHAKEN and STIR framework represents the most promising method for addressing illegal robocalls in the long run, the Commission should not view that framework as the *only* solution. As the Strike Force has pointed out, "the nature of bad actors and their tactics to harass consumers with unwanted robocalls and fraudulent, spoofed Caller IDs are ever changing and adapting."[36] Voice providers thus should be equipped with an array of tools for addressing illegitimate robocalling practices.

1. The Commission Should Empower Providers To Engage in and Collaborate on "Do-Not-Originate" Efforts

Among other things, the Commission should encourage the development and use of industry-wide DNO lists so that voice providers can quickly identify and address illegal spoofed robocalls that use the numbers on these lists. To this end, Comcast supports the Commission's proposal to "codify the clarification contained in the *2016 Guidance PN* that providers may block calls when the subscriber to a particular telephone number requests that calls originating from that number be blocked."[37] Comcast agrees with the *2016 Guidance PN* that such calls should be viewed as "presumptively spoofed and thus likely to violate the Commission's anti-spoofing rules."[38] Moreover, the *2016 Guidance PN* is correct to observe that the "spoofed number's subscriber has a legitimate interest in stopping the spoofed calls – in light of the significant reputational damage and other harms they cause."[39] And "consumers can be presumptively deemed to have consented to the blocking of [such] calls," as no "reasonable

---

36 Oct. 2016 Strike Force Report at 5.

37 *Robocall Blocking NPRM/NOI* ¶ 11; *see also id.* ¶¶ 14-15.

38 *2016 Guidance PN* at 10962.

39 *Id.*

consumer wishes to receive calls that display a spoofed [c]aller ID and have no purpose other than to annoy or defraud."[40]

Consistent with the approach described above in connection with the implementation of SHAKEN and STIR, the Commission should ensure that voice providers have every incentive to embrace and implement this approach and are not deterred from doing so due to regulatory uncertainty. Thus, for instance, call-blocking under this method should be subject to a similar safe harbor in the unlikely event a legitimate call is mistakenly blocked in reliance on a valid DNO request, since absent such a safe harbor, voice providers may be reluctant to take action in response to DNO requests. Provider-initiated blocking in reliance on a valid DNO request also should not count against a provider's call completion rate, for the reasons discussed above in the context of SHAKEN and STIR implementation. And here, too, the Commission should preserve providers' flexibility to implement reasonable tools and not mandate that providers obtain an "opt-in" from subscribers in order to block such calls, given the reasonable presumption that subscribers would prefer not to receive these calls.[41]

Notably, providers have conducted trials employing a DNO list, and as the Strike Force has observed, the results have been impressive. In one trial, the IRS identified numbers that it uses for "inbound-only" purposes and furnished them to participating providers, so that the providers could institute protocols for automatically blocking any calls that appeared to originate from those numbers.[42] During the two-month period in 2016 in which the trial was active, the IRS reported a "90% reduction in IRS scam call complaints, . . . from a high of 43,000

---

40 *Id.*

41 *Robocall Blocking NPRM/NOI* ¶ 25.

42 Oct. 2016 Strike Force Report at 32.

complaints in late August to only 3,700 complaints in mid-October."[43] One Strike Force member also noted a significant reduction in IRS spoofed calls crossing its network, from 8,000 per day to 1,000 per day since the initiation of the trial.

Another trial implemented a DNO list among nine provider networks for a number assigned to a commercial entity whose number was being spoofed with call volumes ranging between just under 400,000 per day to more than one million per day.[44] After all nine providers implemented the DNO list, call volumes dropped to approximately 400 per day.[45] As discussed in the April 2017 Strike Force Report, these DNO trials demonstrate that this method "can be an effective deterrent in mitigating certain types of large and medium scale attacks."[46]

At the same time, any effort to create an industry-wide block list must include a mechanism for sharing information among all providers. As the trial among nine provider networks demonstrated, the ability to share information in a timely and secure manner maximizes the effectiveness of employing a DNO list. Participants in the Strike Force have set up an *ad hoc* shared list of numbers that should not be originated and can add more for review.[47] Going forward, the Commission should encourage providers to establish a robust and scalable platform for sharing these lists on an industry-wide basis—perhaps relying on Internet-based

---

43 *Id.* at 33.

44 *See* Letter of Kevin G. Rupy, Vice President, Law & Policy for the United States Telecom Association, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, at 9 (June 5, 2017).

45 *Id.*

46 Apr. 2017 Strike Force Report at 24.

47 Oct. 2016 Strike Force Report at 32.

mechanisms similar to the manner in which email-related Real-time Block Lists ("RBLs") are shared.[48]

Finally, the Commission should promote efforts to minimize the inadvertent blocking of legitimate callers based on outdated DNO lists. Thus, for instance, individuals and entities that find their numbers on block lists should be afforded a process for removing their numbers from these lists going forward.[49] Similarly, if a voice provider reassigns a number that is on a block list to another subscriber, the provider should update the list to remove the number. Such a process would ensure that robocall mitigation efforts are having their intended effect rather than creating additional frustration for consumers. This process also would appropriately balance the need to address illegitimate robocalling with the need to protect subscribers inadvertently included in providers' robocall mitigation efforts. And such a process would be far easier to administer than the creation of a "white list" mechanism "to enable legitimate callers to proactively avoid having their calls blocked."[50] Based on Comcast's experience in other contexts, maintaining industry-wide white lists that allow individuals or businesses to add their numbers on an *ad hoc* basis can present thorny implementation issues (as opposed to the relatively static white lists that exist for governmental entities like police or fire departments), though individual providers may find it useful to maintain customized white lists and/or subscribe to third-party white list distribution services.

---

48 *See* John Levine, *DNS Blacklists and Whitelists*, Internet Research Task Force (Feb. 2010), *available at* https://tools.ietf.org/html/rfc5782.

49 *See Robocall Blocking NPRM/NOI* ¶¶ 37, 39 (asking whether there should be "a challenge mechanism for callers who may have been blocked in error").

50 *Id.* ¶ 38.

2. *The Commission Should Encourage the Development and Use of Traceback Capabilities*

Another useful approach mentioned in the *Robocall Blocking NPRM/NOI* is the use of increasingly sophisticated "traceback efforts"[51] to gather information about the origin of suspicious calls and about any manipulation of caller ID information along the call path, in an attempt to identify illegal robocalls that should be blocked in the future.[52] The Strike Force has reported on successful trials using traceback information in this manner. In these trials, "the sharing of certain network intelligence and traceback information among [the] participants . . . did lead to the successful thwarting and mitigation of unwanted and illegal phone traffic."[53] The Strike Force Reports also set forth a possible framework for establishing a centralized database in which participating providers can exchange information about illegal calls identified through this method.[54]

As the Strike Force has found, traceback technology and coordination among providers continues to improve, as providers have undertaken significant "investments in personnel and IT systems" and have made "contact information . . . readily available" for personnel to assist with traceback requests.[55] These ongoing efforts will help ensure that providers have put in place "the systems and processes needed to efficiently process requests (whether government subpoenas or requests from other carriers) to identify the source of suspicious traffic traversing their

---

51 The traceback approach is related to but not dependent on SHAKEN and STIR. The SHAKEN and STIR framework includes traceback capabilities, though traceback is possible without implementing SHAKEN and STIR.

52 *Robocall Blocking NPRM/NOI* ¶ 30.

53 Apr. 2017 Strike Force Report at 19.

54 *Id.* at 20-23.

55 *Id.* at 19.

networks."[56] Moreover, the traceback method will become even more streamlined as more providers transition to IP-based networks. Historically, traceback procedures have been "cumbersome in terms of manual investigation of call logs hop by hop."[57] But calls originated in IP format can be tagged with a unique originating identifier that can "make traceback an easy and automatic process."[58]

As with the other methods discussed herein, the Commission should confirm that voice providers may block calls that, based on information obtained through tracebacks, are determined with a reasonably high degree of certainty to be illegal spoofed robocalls. Call-blocking under this method also should be subject to a safe harbor in the unlikely event a legitimate call is mistakenly blocked, and should not count against a provider's call completion totals. And for the same reasons discussed above, the Commission should not require providers to obtain opt-in consent from subscribers in order to block such calls.[59]

3. The Commission Also Should Seek To Promote the Development of Other Objective Criteria To Block Illegal Spoofed Robocalls

The Commission also should remain open to—and not impede—other methods developed by providers for identifying and addressing illegal spoofed robocalls based on objective criteria. Voice providers continue to experiment with various other approaches for combating illegal spoofed robocalls (*e.g.*, reputation-based scoring of telephone numbers, the use of call origination IP addresses to verify authenticity, the establishment of Transport Layer Security certification of calls, etc.), and, in the years to come, providers undoubtedly will

---

56 *Id.*

57 Oct. 2016 Strike Force Report at 9.

58 *Id.*

59 *Robocall Blocking NPRM/NOI* ¶ 25.

develop new and even more effective approaches. At the same time, as the Commission has correctly observed, "illegitimate callers us[e] evolving methods to continue making illegal robocalls" and constantly seek to circumvent the protections that voice providers put in place.[60]

Voice providers must have the flexibility to stay one step ahead of the scammers and implement reasonable call-blocking solutions in response to emerging practices—without the need to wait for regulatory approval to engage in blocking of illegal robocalls every time a new method is invented. Thus, the Commission should strongly consider adopting a rule that affirmatively authorizes voice providers to block calls determined to be illegal spoofed robocalls using *any* reasonable method based on objective criteria, and to establish safe harbors similar to those discussed above for voice providers applying such objective criteria in good faith. Doing so would ensure that regulatory processes do not hamper the development and implementation of such criteria to protect consumers. Indeed, as a policy matter, prior Commission review of these objective criteria is unnecessary, as the interests of consumers, voice providers, and the Commission are in complete alignment when it comes to combatting illegal spoofed robocalls in a manner that prevents harmful communications while ensuring the completion of legitimate calls.[61]

II. OTHER PROPOSALS IN THE NOTICE ARE PROMISING WITH SOME IMPLEMENTATION CHALLENGES

The *Robocall Blocking NPRM/NOI* contains various other proposals targeting specific categories of illegal spoofed robocalls, including calls involving invalid, unallocated, unassigned,

---

60 *Id.*¶ 6.

61 If the Commission believes it is necessary to engage in some review of future methods for addressing illegal spoofed robocalls, it should do so in a way that minimizes delays and avoids disclosing sensitive details of these methods to illegitimate callers—potentially by establishing an expedited process with a clear and predictable timeline in which the Commission can review and bless blocking methods on a confidential basis.

or international numbers.[62] While some of these proposals show immediate promise, others might present potentially significant hurdles to implementation that would need to be overcome, as detailed below. Notably, unlike the SHAKEN and STIR framework discussed above, none of these proposals would provide a mechanism for holistically addressing the vast assortment of illegitimate spoofing conduct faced by consumers today. But some of these proposals likely would enable voice providers to take targeted action in the short term to prevent at least some forms of illegal spoofed robocalling, assuming the implementation issues discussed below can be addressed.

Comcast agrees with the Commission's proposal to "allow[] provider-initiated blocking of calls purportedly originating from numbers that are not valid under the NANP."[63] Of the three specific proposals in the Notice to authorize blocking of illegal robocalls relying on spoofed numbers that are not otherwise in use, this one holds the greatest potential for success in the short term and likely would be the easiest to implement. Voice providers generally have "intimate knowledge of the North American Numbering Plan" and can "easily identify numbers that fall into this category," including numbers that use an N11 code in place of an area code or that repeat a single digit.[64] To be sure, if there are changes to the North American Numbering Plan in the future that alter the set of potentially valid numbers, then voice providers relying on this technique for blocking illegal spoofed robocalls will need to be made aware of these changes. But given that the details of the North American Numbering Plan have always been readily

---

62 *See Robocall Blocking NPRM/NOI* ¶¶ 16-24.

63 *Id.* ¶ 17.

64 *Id.*

available to voice providers, Comcast has no reason to believe that any significant changes to the Plan would go unnoticed.

The Notice also proposes to "allow provider-initiated blocking of calls from numbers that are valid but have not yet been allocated" to a particular provider.[65] That proposal certainly is a logical and laudable extension of the invalid number proposal; after all, as the Notice correctly notes, these valid but unallocated numbers "are similar to invalid numbers in that no subscriber can actually originate a call from any of them," and there is "no legitimate, lawful reason to spoof such a number because they cannot be called back."[66] However, this proposal presents potentially more significant practical challenges. In Comcast's experience, the full set of unallocated numbers is not always evident from the information made available by the North American Numbering Plan Administrator ("NANPA") and the National Number Pool Administrator ("PA").[67] Accordingly, the Commission should couple any action to authorize blocking on this basis with efforts to ensure that NANPA and PA databases (1) more clearly identify which numbers have not yet been allocated and (2) are updated immediately to reflect any new allocations as they occur. Additionally, the Commission should establish a safe harbor for providers attempting to implement blocking on this basis, so that providers are not held liable where a call that is blocked in reliance on these databases turns out to be legitimate.

The Notice's proposal to "allow provider-initiated blocking of calls from numbers that have been allocated to a provider but are not assigned to a subscriber"[68] also poses potentially

---

65 *Id.* ¶ 19.

66 *Id.*

67 The ongoing transition to a new Local Number Portability Administrator ("LNPA") also may present complications for this approach.

68 *Id.* ¶ 21.

thorny implementation issues. A voice provider's assignment of one of its allocated numbers to a subscriber is an internal business decision, and providers typically do not share number assignment information with one another. Moreover, even where voice providers *do* share this information, it becomes stale almost immediately, as providers are constantly assigning new numbers to subscribers or are de-assigning numbers when a subscriber leaves and decides not to take advantage of number portability. While Comcast certainly has interest in exploring the creation of a robust mechanism for aggregating and exchanging this information in a centralized way and in real time, no such mechanism exists today.

Critically, establishing such a mechanism is a prerequisite to implementing an effective solution that allows blocking of calls from allocated but unassigned numbers.[69] Absent a reliable and accepted means for collecting information about number assignments into a centralized database that is constantly updated, there would be a significant risk that legitimate callers would find themselves blocked, particularly those with newly assigned numbers. Moreover, without a way of tracking in real time when previously assigned numbers are no longer assigned to any subscriber, voice providers could not be certain that they are blocking all illegal robocalls that rely on unassigned numbers. And this solution likely would require universal industry participation in order to be maximally effective, as a provider's decision not to participate would create a blind spot in the database. While it may be theoretically possible for the Number Portability Administration Center ("NPAC") to collect and distribute this information, the Commission, in coordination with industry stakeholders, also should explore alternative ways to facilitate real-time information-sharing among voice providers. Moreover, if it intends to adopt this rule, the Commission should consider methods to minimize the potential for abuse when

---

[69] *See id.* ¶ 22.

such information is shared, including by ensuring that access to the database is limited to providers actually participating in the program, and that the use of information in the database is limited to addressing illegal robocalling and not for other commercial purposes.

Finally, as the Commission correctly notes, "internationally originated calls [will] require special treatment."[70] As the Commission hones in on the fraudulent spoofing of domestic calls, much of this illicit activity will move offshore in an effort to circumvent these protective measures—in a manner that, if left unaddressed, could give rise to large-scale abuse. Comcast therefore agrees with the proposal to allow blocking of any "internationally originated call purportedly originated from a NANP number,"[71] as that scenario is akin to allowing blocking of domestically originated calls showing "invalid" numbers. The Commission also should consider specifically authorizing voice providers—to the extent feasible as a technical matter—to allow customers to choose to block international calls altogether or on a country-by-country basis, or to establish a default policy of blocking such calls unless the customer opts out of such blocking.

---

70 *Id.* ¶ 24.

71 *Id.*

CONCLUSION

Illegal spoofed robocalls are a significant and growing problem, and Comcast applauds the Commission's efforts to empower voice providers and consumers to take action to address them. The measures discussed herein will go a long way towards facilitating these efforts, and Comcast looks forward to continuing to work with the Commission and other stakeholders on developing robust and effective solutions in this arena.

Respectfully submitted,

/s/ Kathryn A. Zachem

Kathryn A. Zachem
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

Matthew A. Brill
Matthew T. Murchison
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

July 3, 2017